



GREENBLUM & BERNSTEIN, P.L.C.
Intellectual Property Causes
1950 Roland Clarke Place
Reston, VA 20191
(703) 716-1191

ZW
AR

In re application of: Feng BAO et al.

Attorney Docket No. P19949

Application No. : 09/623,488

Mail Stop Appeal Brief-Patents
 Group Art Unit : 2136

Filed : October 30, 2000

Examiner : P. Parthasarathy

For : A METHOD OF EXCHANGING DIGITAL DATA

Mail Stop Appeal Brief-Patents

Commissioner for Patents
 U.S. Patent and Trademark Office
 Customer Service Window, Mail Stop Appeal Brief-Patents
 Randolph Building
 401 Dulany Street
 Alexandria, VA 22314

Sir:

Transmitted herewith is a **Reply Brief under 37 C.F.R. §41.41** in the above-captioned application.

☐ Small Entity Status of this application under 37 C.F.R. 1.9 and 1.27 has been established by a previously filed statement.

☐ A Request for Extension of Time.

☒ No additional fee is required.

The fee has been calculated as shown below:

Claims After Amendment	No. Claims Previously Paid For	Present Extra	Small Entity		Other Than A Small Entity	
			Rate	Fee	Rate	Fee
Total Claims: 11	*20	0	x25=	\$	x 50=	\$0.00
Indep. Claims: 1	**3	0	x100=	\$	x200=	\$0.00
Multiple Dependent Claims Presented			+180=	\$	+360=	\$0.00
Extension Fees for ___ Month(s)				\$		\$0.00
Total:				\$	Total:	\$0.00

* If less than 20, write 20

** If less than 3, write 3

☐ Please charge my Deposit Account No. 19-0089 in the amount of \$_____.

☒ A check in the amount of \$___ to cover the filing/extension fee is included.

☒ The U.S. Patent and Trademark Office is hereby authorized to charge payment of the following fees associated with this communication or credit any overpayment to Deposit Account No. 19-0089.

☒ Any additional filing fees required under 37 C.F.R. 1.16.

☒ Any patent application processing fees under 37 C.F.R. 1.17, including any required extension of time fees in any concurrent or future reply requiring a petition for extension of time for its timely submission (37 C.F.R. 1.136(a)(3)).

William Pieprz
 Reg. No. 33,630

Bruce H. Bernstein
 Reg. No. 29,027



IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appellant: Feng BAO et al.

Attn: Group Art Unit: 2136

Serial No: 09/623,488

Examiner: P. Parthasarathy

Filed: October 30, 2000

For: A METHOD OF EXCHANGING DIGITAL DATA

REPLY BRIEF UNDER 37 C.F.R. §41.41

Commissioner for Patents
U.S. Patent and Trademark Office
Customer Service Window, Mail Stop Appeal Brief
Randolph Building
401 Dulany Street
Alexandria, VA 22314

Sir :

In response to the Examiner's Answer, dated September 12, 2005, to the Appeal Brief filed March 4, 2005, Appellants submit the present Reply Brief.

Appellants maintains that each reason set forth in the Appeal Brief filed March 4, 2005 for the patentability of the pending claims is correct and again respectfully request that the decision of the Examiner to reject claims 8-18 be reversed and that the application be returned to the Examining Group for allowance.

REMARKS

The "Grounds of Rejection" at page 3 of the Examiner's Answer indicates that the rejections are as set forth in the Final Official Action mailed on August 4, 2004. It is respectfully submitted that the Appeal Brief filed March 4, 2005 has fully addressed the requirements for patentability of the pending claims under 35 U.S.C. §102 and 35 U.S.C. §103. Accordingly, the herein-contained remarks are merely supplemental to the Appeal Brief filed on March 4, 2005. In order to facilitate review of this Reply Brief, the present remarks are limited to a discussion of features of the independent claim of the present application.

However, Appellants initially note that the Examiner's Answer incorrectly asserts, at page 2, that the "rejection of claims 8-18 stands or falls together because appellant's brief does not include a statement that this grouping of claims does not stand or fall together and reasons in support thereof... (See 37 CFR 1.192(c)(7)". The above-noted statement in the Examiner's Answer is in error, as the correct rules that apply to the preparation and filing of Appeal Briefs are found at 37 C.F.R. 41.37, and these rules were in effect at the time the above-noted Appeal Brief was filed on March 4, 2005. In this regard, there is no longer a separate requirement for a statement as to whether a grouping of claims stands or falls together. Further, separate reasons for the patentability of different exemplary claims are provided at, e.g., pages 6-15 (claim 8), page 17-18 (claim 9), page 18 (claims 10 and 15) and pages 18-19 (claim 11). Accordingly, Appellants submit that the claims do not stand and fall together, and that the reasons for the separate patentability of claims, as set forth in the Appeal

Brief dated March 4, 2005, should be given consideration (if necessary) by the Board of Patent Appeals and Interferences.

Rejection Of Claim 8 Under 35 U.S.C. §103(a) Over MICALI In
View Of ANGEBAUD et al

Claim 8 includes features of a "first party encrypting... first digital data and generating an authentication certificate, the authentication certificate authenticating that the encrypted first digital data is an encryption of the first digital data, and sending the encrypted first digital data and the authentication certificate to the second party".

The rejection of claim 8 is based upon the unsupported assertion that an "authentication certificate" may broadly be considered as an "attachment to an electronic message used for security purposes" (see page 4, lines 11-12 of Examiner's Answer). In this regard, the Examiner's Answer asserts, at page 4, second paragraph, that "Appellant recites the limitation with no definition or support for an authentication certificate anywhere in the specification". Appellants submit that this assertion is incorrect, and there is no basis for this broad construction given to the term as first asserted in the Examiner's Answer. In particular, the specification describes, in the context of the claimed invention, an authentication certificate at, e.g., page 9, second paragraph and at page 11, paragraph "(a)".

Additionally, claim 8 itself defines the authentication certificate as "authenticating that the encrypted first digital data is an encryption of the first digital data". It would appear that the definition of "authentication certificate"

asserted in the Examiner's Answer would itself not require the above-noted features, and thus does not itself meet the above-noted limitations recited in claim 8.

Further, as indicated during the prosecution of the present application (e.g., at pages 8-9 of the Response Under 37 C.F.R. §1.116 filed on November 4, 2004), with respect to "An introduction to Public Key Cryptography" (an Exhibit submitted by Appellants during the prosecution of the present application), an authentication certificate "is an assertion of the validity of the binding between the certificate's subject (the owner of the cryptographic keys) and her public key such that other users can be confident that the public key does indeed correspond to the subject who claims it as her own". In contrast to the weight that should be given to the evidence submitted by Appellants, the Examiner has provided no evidentiary basis for her asserted definition of the term "authentication certificate", nor would one of ordinary skill in the art attribute her asserted definition to the term in question, particularly in view of the related recitations in claim 8. In other words, the asserted definition for the term "authentication certificate", as first suggested in the Examiner's Answer, is overly broad, unsupported by any evidence of record and virtually meaningless in the context of the present claims and the applied references.

The rejection of claim 8 is also based on the assertion that MICALI discloses the recited feature of an "authentication certificate authenticating that the encrypted first digital data is an encryption of the first digital data". In this regard, the Examiner's Answer appears to assert, at pages 4 and 5, that the

digital signatures in MICALI disclose the authentication certificate as recited in claim 8. However, as acknowledged by the Examiner at page 4, lines 13-15, what she is considering to be a "(digital) certificate" is that which verifies "that a user sending a message is who he or she claims to be" and that which provides "the receiver with the means to encode a reply". In contrast, the "authentication certificate", as recited in claim 8, authenticates "that the encrypted first digital data is an encryption of the first digital data". In other words, the "authentication certificate" recited in claim 8 is not a mere verification as to the identity of the sender of the message (i.e., a digital signature), and is not a means of providing a receiver with the ability to encode a reply.

Moreover, the Examiner's Answer acknowledges, at page 4, lines 13-15, that she is considering the purported "digital certificate" in MICALI as merely being used to verify that a user sending a message is who he or she claims to be. However, as noted above, even if taken as accurate, what the Examiner considers to be a "digital certificate" in MICALI does not disclose or suggest the "authentication certificate" as recited in claim 8, and is merely a digital signature.

As explained in the Appeal Brief at, e.g., page 7, according to the disclosure of the present invention, the first digital data itself may be a digital signature. Accordingly, there is no basis for any assertion that the claimed "authentication certificate" which accompanies a first digital data in the invention recited in claim 8, is or would be used to perform the same function (to verify the identity of the sender) as the first digital data (a digital signature) itself.

The rejection of claim 8 is also based on the assertion that MICALI discloses a "first party... sending the encrypted first digital data and the authentication certificate to the second party", as recited in claim 8. In particular, in the paragraph bridging pages 4 and 5 of the Examiner's Answer, the Examiner asserts that MICALI discloses at least one communication of a first party to a second party to include generating a digital data string and encrypting the digital data string with an encryption key. However, MICALI discloses only that Bob receives an encryption "z" of a triplet that includes the message "m". Bob cannot verify the message "z" as an encryption of the first digital data "m", and thus does not receive an authentication certificate as recited in claim 8. In particular, the encryption "z" is encrypted in the Post Office's public key of a triplet consisting of identifiers A, B, and the encryption of the message "m" with Bob's public key. In other words, since the encryption of "z" by Alice is performed using an encryption key of a trusted party (i.e., and cannot be opened without the assistance of the trusted party), the purpose of "z" is to identify the sender and to provide a receipt to Bob without providing Bob with an ability to verify the contents (yet). This is, in fact, consistent with the Examiner's own acknowledgement, at page 4, lines 13-15 of the Examiner's Answer, where she acknowledges considering a digital certificate only as being well known for use to verify that a user sending a message is who he or she claims to be. Accordingly, the encryption for "z" is not the "authentication certificate" recited in claim 8, and does not accompany the "authentication certificate" recited in claim 8.

If Alice receives the properly signed receipt $SIG_B(z)$ from Bob at step A2, Alice sends Bob the original message "m" encrypted using only Bob's public key (i.e., $E_B(m)$) so that Bob can decrypt the message. Accordingly, Alice receives a receipt for what she sent to Bob and Bob receives the information $E_B(m)$. Of course, if Bob cannot verify $E_B(m)$ at step B2, Bob sends the original value "z" to the Post Office, and the Post Office decrypts "z" to obtain $E_B(m)$. Therefore, Alice sends Bob the message $E_{PO}((A, B, E_B(m)))$, and Bob sends Alice a signed receipt for $E_{PO}((A, B, E_B(m)))$.

With respect to the use of digital signatures in MICALI, MICALI discloses, at column 6, lines 1-5, that Alice can digitally sign "z", i.e., to obtain $SIG_A(z)$. However, $SIG_A(z)$ is not used by Bob to verify that the encrypted first digital data (i.e., "z") is an encryption of the first digital data (i.e., "m"). Rather, Bob may use Alice's public key to decrypt $SIG_A(z)$ and determine that Alice is the sender (see MICALI, column 6, lines 1-7). Thus, Alice's signature of "z" allows Bob to verify the origin of the message, but provides no assurance to Bob that "z" is an encryption of the first digital data.

In contrast, the authentication certificate of the present invention authenticates that the encrypted first digital data is an encryption of the first digital data. Thus, Alice's digital signature in MICALI does not and cannot obtain the same result for Bob as the authentication certificate recited in claim 8 obtains for the second party.

In other words, MICALI does not disclose, suggest or render obvious an "authentication certificate", let alone an "authentication certificate authenticating

that the encrypted first digital data is an encryption of the first digital data". Further, MICALI does not disclose, suggest or render obvious "the first party... sending the encrypted first digital data and the authentication certificate to the second party".

Accordingly, there is no proper basis for any assertion that the above-noted combination of features recited in claim 8 are disclosed, suggested or rendered obvious in PETT.

Claim 8 also includes a recitation of "the second party verifying that the encrypted first digital data is an encryption of the first digital data using the authentication certificate, and the second party sending the second digital data to the first party when the encrypted first digital data is an encryption of the first digital data".

The rejection of claim 8 is based upon the assertion that the above-noted features are disclosed by MICALI at column 5, line 50 to column 6, line 21 and column 6, lines 34-61 (see Examiner's Answer, page 5, lines 10-11) . In this regard, it is not clear which element in MICALI the Examiner is referring to as the authentication certificate.

However, the encrypted data string sent from Alice to Bob at step B1 is "z", and Bob simply signs "z" and sends it to Alice as the receipt without authenticating "z". In other words, the encrypted data string "z" which is sent from Alice to Bob is not itself an "authentication certificate", and is not accompanied by an "authentication certificate". MICALI does not disclose the use of an "authentication certificate", let alone that Bob verifies "that the

encrypted first digital data is an encryption of the first digital data using the authentication certificate". Rather, MICALI discloses that Bob signs "z" and sends the signed "z", i.e., "SIG_B(z)" to Alice at step B1.

Additionally, there is no verification at step A2 when Alice sends E_B(m) to Bob. In this regard, and as explained above, no verification is necessary at step A2 because Bob merely uses his own private key to decrypt E_B(m) to obtain the message "m". Accordingly, if Bob has obtained the message "m" at step A2, there would be no motivation to modify MICALI, with ANGEBAUD or any other reference. In this regard, there would be no purpose to having Alice send a separate authentication certificate to Bob when Bob already has the clear message "m" which was encrypted only in his own key as E_B(m).

Further, as explained above, if Alice signed "z", then Bob may use Alice's public key to decrypt SIG_A(z) and determine that Alice is the sender (see MICALI, column 6, lines 1-7). Thus, Alice's signature of "z" allows Bob to verify the origin of the message, but provides no assurance to Bob that "z" is an encryption of the first digital data.

Further, there is no disclosure in MICALI of a "second party sending the second digital data to the first party when the encrypted first digital data is an encryption of the first digital data". Rather, as explained in the Appeal Brief at page 11, lines 3-8, Bob signs the message and sends the signed message SIG_B(z) back to Alice regardless of whether the message "m" is worthless or valuable (i.e., without verifying that "z" is an encryption of "m" in MICALI).

Appellants further submit that the above-noted features are not disclosed or suggested by ANGEBAUD; nor has the Examiner asserted at any time that the above-noted features are disclosed or suggested by ANGEBAUD. In this regard, it is still not clear what modifications to MICALI the Examiner would even admit are necessary to obtain the invention recited in claim 8. Accordingly, because the combination of references applied by the Examiner do not disclose, suggest or render obvious the features recited in claim 8, Appellants respectfully submit that the rejection of claim 8 is inappropriate.

Accordingly, the rejection of claim 8 under 35 U.S.C. §103(a) over MICALI in view of ANGEBAUD is improper and should be reversed.


CONCLUSION

As noted previously, the above remarks are limited to a discussion of features of the independent claim of the present application. In this regard, separate arguments were set forth for the patentability of various of the dependent claims in the Appeal Brief filed on March 4, 2005, and each of the reasons for allowability of both independent claims and dependent claims, as set forth in the Appeal Brief filed on March 4, 2005, is correct.

Accordingly, each and every pending claim of the present application meets the requirements for patentability under 35 U.S.C. §103, and the present application and each pending claim therein are allowable over the prior art of record.

Should there be any questions, any representative of the U.S. Patent and Trademark Office is invited to contact the undersigned at the below-listed telephone number.

Respectfully submitted,
Feng BAO et al.



Bruce H. Bernstein
Reg. No. 29,027

William Pieprz
Reg. No. 33,630

November 7, 2005
GREENBLUM & BERNSTEIN, P.L.C.
1950 Roland Clarke Place
Reston, VA 20191
(703) 716-1191